DEPARTMENT OF THE AIR FORCE
HEADQUARTERS AIR COMBAT COMMAND
LANGLEY AIR FORCE BASE VIRGINIA

27 JUL 2004

MEMORANDUM FOR HQ ACC/SG

FROM: HQ ACC/SCS

SUBJECT: Addendum 1 to ACC Interim Approval to Operate (ICtO) and Interim Approval to Operate (IAtO) for MHS Management Analysis and Reporting Tool (MHS MART or M2) (25 Nov 03) for MART/M2 version 3.0

1. In accordance with AFPD 33-2, *Information Protection* and ACCI 33-174, *Certifying the ACC Enterprise*, I issue an addendum to ACC ICtO and IAtO for MHS MART/M2 (25 Nov 03) and authorize the use of MART/M2 version 3.0 to include the use of the Full Client Interface. This approval allows the system to operate at all ACC bases up to the sensitive, unclassified level in the system high security mode of operation. The Designated Approving Authority's (DAA) review of the Systems Security Authorization Agreement (SSAA) verifies that sufficient system security countermeasures have been implemented and an acceptable level of protection exists. The original expiration date, 24 Nov 04, of the DAA approved accreditation does not change.

2. The assigned Information Systems Security Officer (ISSO) is required to follow the SSAA and DAA provided guidance throughout the life cycle of the system. The ACC Network Operations and Security Center will inform the local Network Control Center that the system is authorized for use on the ACC Enterprise. Before system activation, the functional information system's owner and the host wing Information Assurance Office will complete the ACC Site Certification Checklist. The ISSO maintains the completed checklist and SSAA for the system's life cycle.

3. This ICtO and IAtO are only valid for the current version's system software configuration and associated hardware. Any changes to this system (i.e. revisions, upgrades, or new versions) will nullify this approval. Please contact your ACC/SCS IT consultant, Mr. Mainvielle, HQ ACC/SCSO, DSN 574-5005, if you have any questions.

STEVEN N. SIMKINS, GS-14, DAF
Deputy Chief, Systems Integration Division
Directorate, Communications and Information Systems

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS AIR COMBAT COMMAND
LANGLEY AIR FORCE BASE, VIRGINIA

MEMORANDUM FOR HQ ACC/SCS

FROM: HQ ACC/SCSC

SUBJECT: Recommendation for an Addendum 1 to ACC Interim Approval to Operate (ICtO) and Interim Approval to Operate (IAtO) for MHS Management Analysis and Reporting Tool (MHS MART or M2) (25 Nov 03) for MART/M2 version 3.0

1. The Medical Health System (MHS) MART/M2 supports the storage, reporting, and analysis of medical operations data gathered from various source systems with the MHS domains. An ICtO and IAtO for MART/M2 was issued on 25 Nov 03 with the stipulation that they could not use the Full Client Interface (FCI) to access data. This stipulation was due to the fact that the FCI accessed data in clear text communications.

2. MART/M2 has implemented an AF VPN solution to resolve the M-2 encryption issues. All AF M2 user data traffic is routed to the AF VPN located at the SSG in Montgomery, AL and encryption will terminate at the AF VPN router in DECC-D Denver. AFCA/GCLD confirmed the AF VPN solution has been installed at the SSG Montgomery, AL and DECC-D Denver. Therefore, the data now transmitted with the FCI is encrypted. After complete review and evaluation of the available documentation, we recommend an **Addendum to ACC ICtO and IAtO for MHS MART/M2 (25 Nov 03) for MART/M2 with FCI in the system high security mode of operation up to the sensitive, unclassified level**.

3. Residual risks remain from the original IAtO. All remaining risks can be grouped into three main categories, summarized below. A detailed breakdown of residual risk is attached.

a. Risks with No Countermeasures: These are all the risks without any realistic countermeasures available. There may be certain limitations and constraints imposed to help mitigate these risks to an acceptable level.

b. Risks with Insufficient Countermeasures: These are all the risks with countermeasures applied, however, the countermeasures do not fully mitigate the risk. Countermeasures to further reduce risk may be unavailable or not economically feasible.

c. Mitigated Risks: These risks are deemed to have been reduced to a level where they no longer pose a measurable risk to system operation. They were presented as risks in the system certification package (identified during the risk analysis process or security test and evaluation), however, applied countermeasures or imposed limitations and constraints nullify these risks.

THOMAS H. FLOYD, JR, GS-12, DAF
Acting Chief, IT Assessment Branch
Directorate, Communications and Information Systems

SITE CERTIFICATION CHECKLIST

Management and Analysis and Reporting Tool (MART/M2) Version 3.0

	Completed	N/A
Site Security Personnel		
1. Identify Local Certification Authority.		
2. Notify Wing Information Assurance Office of impending installation.		
3. Assign other system security officials, (i.e. ISSO, SA, FSA, …) and document in writing.		
Documentation		
1. Ensure local personnel possess a copy of the Certificate to Operate (CtO) package to include SSAA, DAA letter, and Breakdown of Residual Risks.		
2. Install AIS or application as described in the CtO package.		
3. Document a list of all hardware variances. If there are variances do not implement until a change request is validated by the Certifying Authority and approved by MAJCOM DAA		
4. Document a list of all software variances. If there are variances, do not implement until a change request is validated by the Certifying Authority and is approved by MAJCOM DAA		
5. Include a diagram of the system network if adding systems. Submit diagram with completed checklist.		
6. Document any site-specific security policies that are not already in the System Security Policy. If there are changes to the security policies do not implement until a change request is validated by the Certifying Authority and approved by MAJCOM DAA.		
7. Document any site-specific additions/deletions to the Threat/Vulnerability Matrix.		
Certification		
1. Perform any countermeasures identified in Risk Analysis section of SSAA and ACC Breakdown of Residual Risk.		
2. Verify system integrity by running an ISS scan. Correct and identify any additional vulnerabilities.		
3. If the AIS connects two or more different security classification networks, it must use an approved Secret and Below Interoperability (SABI) solution and receive final SABI board approval before operational use.		
4. Return this completed checklist to SCS.		

Certifying Authority's Validation

Date Submitted: ____________________

Signature: ______________________________

Name: ________________________________

Title: ________________________________